AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (currently amended): An authentication method ~~at~~ for a wireless LAN (local area network) system, comprising ~~the steps of~~:

transmitting an authentication request from a STA (terminal station) to an AP (access point), with which said STA desires to make association;

requesting authentication of said authentication request from said AP to an authentication server, by converting said authentication request to a protocol adaptable to said authentication server;

~~cheking~~ checking said authentication request at said authentication server based on a MAC (media access control) address of said STA;

executing encryption authentication at said AP with said STA based on a designated encryption algorithm; and

notifying an authentication completion from said authentication server to said AP, after said authentication server received a response of a completion of said encryption authentication from said AP.

2. (currently amended): An authentication method ~~at~~ for a wireless LAN system in accordance with claim 1, wherein:

after said encryption authentication is normally completed, a table of said MAC address in said AP is renewed by an instruction from said authentication server.

3. (currently amended): An authentication method ~~at~~ for a wireless LAN system in accordance with claim 1, wherein:

in case that a trouble occurs at said authentication server, said AP itself executes authentication of said MAC address.

4. (currently amended): An authentication method ~~at~~ for a wireless LAN system in accordance with claim 1, wherein:

said encryption algorithm uses a shared key having a predetermined usable period.

5. (currently amended): An authentication method ~~at~~ for a wireless LAN system in accordance with claim 4, wherein:

in case that said predetermined usable period of said shared key expired, said MAC address is authenticated by an open system authentication method; and

wherein at said open system authentication method, after association, a period of communication is limited to a designated short time, and a key is transported in said limited time by using such an Internet Key Exchange method of Public Key Infrastructure, and said authentication request is executed again by using said shared key.

6. (currently amended): An authentication apparatus ~~at~~ for a wireless LAN system, comprising:

plural STAs;

plural APs which connect to an authentication server and said plural STAs, and one of said plural APs receives an authentication request from one of said plural STAs and converts said authentication request from one of said plural STAB to a protocol adaptable to said authentication server, and authenticates said authentication request from one of said plural STAs based on a designated encryption algorithm; and

said authentication server which checks said authentication request from one of said STAs based on a MAC address of one of said plural STAs by receiving said converted authentication request, and notifies an authentication completion to said AP, after said authentication server received a response of a completion of encryption

authentication from said AP.

7. (currently amended): An authentication apparatus ~~at~~ for a wireless LAN system in accordance with claim 6, further comprising:

a renewing means for renewing a table of said MAC address in said AP by an instruction from said authentication server, after said encryption authentication is normally completed.

8. (currently amended): An authentication apparatus ~~at~~ for a wireless LAN system in accordance with claim 6, wherein:

in case that a trouble occurs at said authentication server, said AP itself executes authentication of said MAC address.

9. (currently amended): An authentication apparatus ~~at~~ for a wireless LAN system in accordance with claim 6, wherein:

said authentication algorithm is a WEP (wired equivalent privacy) algorithm stipulated in the IEEE 802.11.

10. (currently amended): An authentication apparatus ~~at~~ for a wireless LAN system in accordance with claim 6, wherein:

said encryption algorithm uses a shared key having a predetermined usable period.

11. (currently amended): An authentication apparatus ~~at~~ for a wireless LAN system in accordance with claim 10, wherein:

in case that said predetermined usable period of said shared key expired, said MAC address is authenticated by an open system authentication method; and

wherein at said open system authentication method, after association, a period of communication is limited to a designated short time, and a key is transported in said limited time by using such an Internet Key Exchange method of Public Key Infrastructure, and said authentication request is executed again by using said shared key.

12. (new): A wireless and fixed-line interface apparatus comprising:

a first authentication part for executing an authentication based on a first information certificate provided by a terminal;

a second authentication part for executing an authentication based on a second information certificate provided by said terminal;

a storing part for storing said second information certificate, which is used for authenticating said terminal; and

a communication part for communicating with an authentication server;

wherein said communication part requests from said authentication server an authentication based on said second information certificate, and

said second authentication part executes an authentication in accordance with a response from said authentication server.

13. (new): An access point in a wireless LAN system comprising:

a first authentication part for executing an authentication based on a first information certificate provided by a terminal;

a second authentication part for executing an authentication based on a second information certificate provided by said terminal;

a storing part for storing said second information certificate, which is used for authenticating said terminal; and

a communication part for communicating with an authentication server,

wherein said communication part requests from an authentication server an authentication based on said second information certificate , and

according to a response from said authentication server, said second authentication part determines whether to permit, or not to permit, said terminal to connect with a network.

14. (new): An access point apparatus comprising:

a first authentication part for executing an encrypted authentication of a terminal; and

a second authentication part for executing a MAC address authentication of said terminal, using information about a MAC address, which is possessed by an authentication server.

15. (new): An access point apparatus comprising:

a first authentication part for executing an encrypted authentication of a terminal;

a second authentication part for executing a MAC address authentication of said terminal; and

a storing part for storing a MAC address, which is used for executing a MAC address authentication of said terminal,

wherein when a connection request is issued from said terminal, said second authentication part authenticates said terminal, using said MAC address stored by said storing part and using information possessed by an authentication server, which issues permission for establishing a connection.

16. (new): An access point apparatus comprising:

an authentication part for executing an encrypted authentication of a terminal;

a communication part for communicating with an authentication server which manages the MAC address of said terminal; and

a connection control part for controlling a connection of said terminal to a network,

wherein when an authentication request is issued from said terminal:

said authentication part authenticates said terminal;

said communication part sends the MAC address of said terminal to said authentication server and receives a result of a MAC address authentication performed by said authentication server; and

said connection control part permits said terminal to connect with a network when said MAC address authentication succeeds, and does not permit said terminal to connect with a network when said MAC address authentication fails.

17. (new): An access point apparatus comprising:

an authentication part for executing an encrypted authentication of a terminal;

a communication part for querying an authentication server about a MAC address of said terminal;

a connection control part for allowing said terminal to connect with a network when a MAC address of said authentication server coincides with that of said terminal.

18. (new): An access point apparatus comprising:

a first authentication part for performing an encrypted authentication of a terminal using a WEP algorithm; and

a second authentication part for performing a MAC address authentication of said terminal,

wherein when an authentication request is issued by said terminal, an authentication is performed by said first authentication part and said second authentication part, and

communication is established with an authentication server, which determines whether to permit, or not to permit, said terminal to connect with a network according to said MAC address of said terminal.

19. (new): An access point apparatus comprising:

a first authentication part for performing an encrypted authentication of a terminal using a WEP algorithm;

a second authentication part for performing a MAC address authentication of said terminal; and

a storing part for storing a MAC address of said terminal,

wherein when a connection request is issued from said terminal, said first authentication part and said second authentication part perform authentications, and said second authentication part also uses MAC address stored in an authentication server.

20. (new): An access point apparatus in a wireless LAN system comprising:

a first authentication part for executing at least one of an encrypted authentication and an open system authentication of a terminal; and

a second authentication part for executing an authentication of said terminal using information of a MAC address of said terminal,

wherein said second authentication part also uses MAC address stored in an authentication server, which manages MAC addresses of terminals placed in one wireless LAN system, in executing an authentication of said terminal.

21. (new): A wireless LAN system comprising

a terminal

an access point apparatus; and

an authentication server,

wherein said terminal comprises a communication part for wirelessly communicating with said authentication server,

wherein said access point apparatus comprises

a first authentication part for executing an encrypted authentication of a terminal and a second authentication part for executing a MAC address authentication of said terminal, and

wherein said authentication server comprises a storing part for storing a MAC address of a terminal and a responding part for responding to an inquiry of said access point apparatus about a MAC address.

22. (new): A wireless LAN system comprising

a terminal;

an access point apparatus; and

an authentication server,

wherein said terminal comprises a communication part for wirelessly communicating with said access point apparatus,

wherein said access point apparatus performs an encrypted authentication of a terminal and performs a MAC address authentication of said terminal, and

wherein said authentication server stores a MAC address of said terminal and supports the MAC address authentication with the stored MAC address.

23. (new): A wireless LAN system comprising:

a terminal;

an access point apparatus; and

an authentication server,

wherein said terminal comprises a communication part for wirelessly communicating with said access point apparatus,

wherein said access point apparatus comprises an authentication part for performing a MAC authentication of said terminal, and

wherein said authentication server, which is placed in one wireless LAN system where roaming is not needed, comprises a storing part for storing a MAC address of said terminal and a

responding part for responding to an inquiry from said access point apparatus about MAC address.

24. (new): An authentication server used in a wireless LAN system, comprising:

plural STAs;

plural APs which connect to an authentication server and said plural STAs, and one of said plural APs receives an authentication request from one of said plural STAs and converts said authentication request from one of said plural STAB to a protocol adaptable to said authentication server, and authenticates said authentication request from one of said plural STAs based on a designated encryption algorithm; and

said authentication server which checks said authentication request from one of said STAs based on a MAC address of one of said plural STAs by receiving said converted authentication request, and notifies an authentication completion to said AP, after said authentication server received a response of a completion of encryption authentication from said AP,

wherein said encryption algorithm uses a shared key having a predetermined usable period,

wherein in case that said predetermined usable period of said shared key expired, said MAC address is authenticated by an open system authentication method; and

wherein at said open system authentication method, after association, a period of communication is limited to a designated short time, and a key is transported in said limited time

by using such an Internet Key Exchange method of Public Key Infrastructure, and said authentication request is executed again by using said shared key.

25. (new): An authentication server used in a wireless or a fixed-line interface apparatus comprising:

a first authentication part for executing an authentication based on a first information certificate provided by a terminal;

a second authentication part for executing an authentication based on a second information certificate provided by said terminal;

a storing part for storing said second information certificate, which is used for authenticating said terminal; and

a communication part for communicating with an authentication server;

wherein said communication part requests from said authentication server an authentication based on said second information certificate, and

said second authentication part executes an authentication in accordance with a response from said authentication server.

26. (new): A terminal used in a wireless LAN system comprising:

plural STAs;

plural APs which connect to an authentication server and said plural STAs, and one of said plural APs receives an authentication request from one of said plural STAs and converts said authentication request from one of said plural STAB to a protocol adaptable to said

authentication server, and authenticates said authentication request from one of said plural STAs based on a designated encryption algorithm; and

said authentication server which checks said authentication request from one of said STAs based on a MAC address of one of said plural STAs by receiving said converted authentication request, and notifies an authentication completion to said AP, after said authentication server received a response of a completion of encryption authentication from said AP,

wherein said encryption algorithm uses a shared key having a predetermined usable period,

wherein in case that said predetermined usable period of said shared key expired, said MAC address is authenticated by an open system authentication method; and

wherein at said open system authentication method, after association, a period of communication is limited to a designated short time, and a key is transported in said limited time by using such an Internet Key Exchange method of Public Key Infrastructure, and said authentication request is executed again by using said shared key.

27. (new): A terminal used in a wireless or a fixed-line interface apparatus comprising:

a first authentication part for executing an authentication based on a first information certificate provided by a terminal;

a second authentication part for executing an authentication based on a second information certificate provided by said terminal;

a storing part for storing said second information certificate, which is used for authenticating said terminal; and

a communication part for communicating with an authentication server;

wherein said communication part requests from said authentication server an authentication based on said second information certificate, and

said second authentication part executes an authentication in accordance with a response from said authentication server.

28. (new): A method for authenticating a terminal in a wireless LAN system including a terminal, an access point apparatus, and an authentication server, comprising:

performing, by said access point apparatus, an encrypted authentication and a MAC address authentication of said terminal when an authentication request is issued from said terminal;

inquiring, by said access point apparatus, to said authentication server whether said terminal is permitted, according to a MAC address, to communicate;

performing, by said access point apparatus, a MAC address authentication of said terminal according to a response to said inquiry.

29. (new): A method for authenticating a terminal in a wireless LAN system comprising:

performing, by an access point apparatus, an encrypted authentication of a terminal when an authentication request is issued from said terminal; and

performing a MAC address authentication of said terminal with the MAC address information that an authentication server manages.

30. (new): An authentication method for a wireless LAN system in accordance with claim 1, wherein said authentication request from said STA to said AP comprises a request to establish an authorized connection with said AP for the exchange encrypted data.

31. (new): An authentication method for a wireless LAN system in accordance with claim 1, wherein said authentication server comprises data relating to more than 10,000 MAC addresses.